Claims 1-23 were rejected under 35 U.S.C. Section 112. Claim 9 was objected to because of an informality. Appropriate corrections and clarifications have been made.

Claims 1-23 were also provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-33 of copending Application No. 10683579. An appropriate Terminal Disclaimer is being submitted with this response.

Corrected drawing sheets (Replacement Sheets) to correct misspellings in FIG. 13 and FIG. 14 are being submitted with this response

Claims 1-23 were also rejected under 35 U.S.C. 102(b) as being anticipated by *Togawa* et al. (U.S. Pat. No. 5,918,008). .
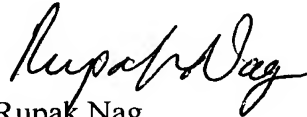
Claims 1, 10, and 17 have been amended to recite that when the virus sensor (in the virus monitor) operates in a first mode or stand-by mode, it does not affect the bandwidth or speed of the traffic flowing through the network because in this mode data packets are not removed from or added to network traffic, but rather are copied and the copies of the data packets, not the actual packets themselves, are analyzed by the virus sensor. When the virus sensor switches to a second mode or inline mode, the data packets are not copied but rather the actual packets are analyzed. Those data packets determined to be infected or suspected of being infected are not returned to the network. The claims also recite that the virus monitor collects network environment data and assigns an IP address to itself. It also locates a controller in the network and registers itself with the controller, from where it receives a rule set and an outbreak prevention policy (OPP). Support for these amendments can be found in the discussion, for example, of Figures 2 and 5 in the specification.

In contrast, the *Togawa* reference describes a storage device having various means, such as an infection management table means to manage files on a disk and determine if files are

infected. Also described are a table registration means, a virus checker to determine whether a file is infected, and means for keeping infected files from being distributed or used by external components. It does not describe a virus monitor having a virus sensor as claimed. For example, it does not teach or describe a mode where data packets are copied so that network bandwidth is not adversely affected. Nor does it describe or anticipate another mode where the copying function ceases when a virus is detected or suspected in data packets and those data packets are restricted from re-entering network traffic. In another example, the means or components in the storage device described in *Togawa* do not enable the device to collect network environment data or registering with a controller (or any network component) from which it receives, for example, a rule set (related to virus protection) or an "outbreak prevention policy."

Applicant believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER LLP

Rupak Nag
Reg. No. 37,493

P.O. Box 70250
Oakland, CA 94612-0250
Telephone: (612) 252-3335